Manufacturer Disclosure Statement for Medical Device Security – MDS²

DEVICE DESCRIPTION

Device Category	Manufacturer	Document ID	Document Release Date
Hearing Aid Analyzer	Audioscan		

Device Model	Software Revision		Software Release Date
Verifit 2 / Axiom	See Page 1 of Users Guide		See Page 1 of Users Guide

Manufacturer or Representative Contact Information	Company Name	Manufacturer Contact Information
	Audioscan, a div. of Etymonic Design Inc.	support@audioscan.com
	Representative Name/Position	1-800-265-2093
	Chris McInerney, Product Manager	

Intended use of **device** in network-connected environment:

MANAGEMENT OF PRIVATE DATA

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.

			Yes, No, N/A, or See Note	Note #
A	Can this **device** display, transmit, or maintain **private data** (including **electronic Protected Health Information** [ePHI])?		No	1
B	Types of **private data** elements that can be maintained by the **device**:			
	B.1	Demographic (e.g., name, address, location, unique identification number)?	No	__
	B.2	Medical record (e.g., medical record #, account #, test or treatment date, **device** identification number)?	No	__
	B.3	Diagnostic/therapeutic (e.g., photo/radiograph, test results, or physiologic data with identifying characteristics)?	No	__
	B.4	Open, unstructured text entered by **device user/operator**?	Yes	1
	B.5	**Biometric data**?	No	__
	B.6	Personal financial information?	No	__
C	Maintaining **private data** - Can the **device**:			
	C.1	Maintain **private data** temporarily in volatile memory (i.e., until cleared by power-off or reset)?	Yes	_2_
	C.2	Store **private data** persistently on local media?	Yes	1
	C.3	Import/export **private data** with other systems?	Yes	3
	C.4	Maintain **private data** during power service interruptions?	No	__
D	Mechanisms used for the transmitting, importing/exporting of **private data** – Can the **device**:			
	D.1	Display private data (e.g., video display, etc.)?	No	__
	D.2	Generate hardcopy reports or images containing **private data**?	Yes	1
	D.3	Retrieve **private data** from or record **private data** to **removable media** (e.g., disk, DVD, CD-ROM, tape, CF/SD card, memory stick, etc.)?	Yes	1
	D.4	Transmit/receive or import/export **private data** via dedicated cable connection (e.g., IEEE 1073, serial port, USB, FireWire, etc.)?	No	__
	D.5	Transmit/receive **private data** via a wired network connection (e.g., LAN, WAN, VPN, intranet, Internet, etc.)?	Yes	_1_ 3,4
	D.6	Transmit/receive **private data** via an integrated wireless network connection (e.g., WiFi, Bluetooth, infrared, etc.)?	Yes	_
	D.7	Import **private data** via scanning?	No	__
	D.8	Other?	____	__

Management of Private Data notes:

1. The device does not create, store, transmit, or otherwise require the use of ePHI. However, the operator may enter free-form text when saving or printing data. If patient-identifable information is manually added in this fashion, ePHI is created when this data is stored to a USB stick or network file. Users are recommended to take care to not enter private data.

2. If an operator enters a header for printing, that header will remain on the machine until it is cleared or overwritten.

3. The device can import and export data and headers that may include ePHI, but only in the event that ePHI was entered by the operator. The device can import/export via network connection or transfer via USB stick.

4. Device is capable of wireless 802.11 network connection.

Device Category	Manufacturer	Document ID	Document Release Date
Hearing Aid Analyzer	Audioscan		

Device Model	Software Revision		Software Release Date
Verifit 2	See Page 1 of Users Guide		See Page 1 of Users Guide

SECURITY CAPABILITIES

	Yes, No, N/A, or See Note	Note #
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		

1   AUTOMATIC LOGOFF (ALOF)

The **device**'s ability to prevent access and misuse by unauthorized **users** if **device** is left idle for a period of time.

1-1 Can the **device** be configured to force reauthorization of logged-in **user**(s) after a predetermined length of inactivity (e.g., auto-logoff, session lock, password protected screen saver)?	No	__
1-1.1 Is the length of inactivity time before auto-logoff/screen lock **user** or administrator configurable? (Indicate time [fixed or configurable range] in notes.)	No	__
1-1.2 Can auto-logoff/screen lock be manually invoked (e.g., via a shortcut key or proximity sensor, etc.) by the **user**?	No	__

ALOF notes:

2   AUDIT CONTROLS (AUDT)

The ability to reliably audit activity on the **device**.

2-1 Can the **medical device** create an **audit trail**?	No	__
2-2 Indicate which of the following events are recorded in the audit log:		
2-2.1 Login/logout	N/A	__
2-2.2 Display/presentation of data	N/A	__
2-2.3 Creation/modification/deletion of data	N/A	__
2-2.4 Import/export of data from **removable media**	N/A	__
2-2.5 Receipt/transmission of data from/to external (e.g., network) connection	N/A	__
2-2.5.1 **Remote service** activity	N/A	__
2-2.6 Other events? (describe in the notes section)	N/A	__
2-3 Indicate what information is used to identify individual events recorded in the audit log:		
2-3.1 **User** ID	N/A	__
2-3.2 Date/time	N/A	__

AUDT notes:

3   AUTHORIZATION (AUTH)

The ability of the device to determine the authorization of users.

3-1 Can the **device** prevent access to unauthorized **users** through **user** login requirements or other mechanism?	No	__
3-2 Can **users** be assigned different privilege levels within an application based on 'roles' (e.g., guests, regular **users**, power **users**, administrators, etc.)?	No	__
3-3 Can the **device** owner/**operator** obtain unrestricted administrative privileges (e.g., access operating system or application via local root or admin account)?	No	__

AUTH notes:

Device Category	Manufacturer	Document ID	Document Release Date
Hearing Aid Analyzer	Audioscan		

Device Model	Software Revision		Software Release Date
Verifit 2	See Page 1 of Users Guide		See Page 1 of Users Guide

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

4   CONFIGURATION OF SECURITY FEATURES (CNFS)

The ability to configure/re-configure **device security capabilities** to meet **users'** needs.

4-1 Can the **device** owner/operator reconfigure product **security capabilities**?	No	__

CNFS notes:

5   CYBER SECURITY PRODUCT UPGRADES (CSUP)

The ability of on-site service staff, remote service staff, or authorized customer staff to install/upgrade **device's** security patches.

5-1 Can relevant OS and **device** security patches be applied to the **device** as they become available?	No	5
5-1.1 Can security patches or other software be installed remotely?	No	__

CSUP notes:

5. There is no virus protection software available for the device; it is not required as it is not possible to load or execute software on the device except that which is provided by the manufacturer. User has no console access to operating system.

6   HEALTH DATA DE-IDENTIFICATION (DIDT)

The ability of the **device** to directly remove information that allows identification of a person.

6-1 Does the **device** provide an integral capability to de-identify **private data**?	Yes	__

DIDT notes:

7   DATA BACKUP AND DISASTER RECOVERY (DTBK)

The ability to recover after damage or destruction of **device** data, hardware, or software.

7-1 Does the **device** have an integral data backup capability (i.e., backup to remote storage or **removable media** such as tape, disk)?	No	__

DTBK notes:

8   EMERGENCY ACCESS (EMRG)

The ability of **device users** to access **private data** in case of an emergency situation that requires immediate access to stored **private data**.

8-1 Does the **device** incorporate an **emergency access** ("break-glass") feature?	No	__

EMRG notes:

9   HEALTH DATA INTEGRITY AND AUTHENTICITY (IGAU)

How the **device** ensures that data processed by the **device** has not been altered or destroyed in an unauthorized manner and is from the originator.

9-1 Does the **device** ensure the integrity of stored data with implicit or explicit error detection/correction technology?	No	__

IGAU notes:

Device Category	Manufacturer	Document ID	Document Release Date
Hearing Aid Analyzer	Audioscan		

Device Model	Software Revision		Software Release Date
Verifit 2	See Page 1 of Users Guide		See Page 1 of Users Guide

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

10   MALWARE DETECTION/PROTECTION (MLDP)

The ability of the **device** to effectively prevent, detect and remove malicious software (**malware**).

10-1 Does the **device** support the use of **anti-malware** software (or other **anti-malware** mechanism)?	No	6
10-1.1 Can the **user** independently re-configure **anti-malware** settings?	N/A	__
10-1.2 Does notification of **malware** detection occur in the **device user** interface?	N/A	
10-1.3 Can only manufacturer-authorized persons repair systems when **malware** has been detected?	N/A	__
10-2 Can the device owner install or update **anti-virus software**?	N/A	__
10-3 Can the device owner/**operator** (technically/physically) update virus definitions on manufacturer-installed **anti-virus software**?	No	6

MLDP notes: 6. There is no virus protection software available for the device; it is not required as it is not possible to load or execute software on the device except that which is provided by the manufacturer.

11   NODE AUTHENTICATION (NAUT)

The ability of the **device** to authenticate communication partners/nodes.

11-1 Does the **device** provide/support any means of node authentication that assures both the sender and the recipient of data are known to each other and are authorized to receive transferred information?	No	__

NAUT notes:

12   PERSON AUTHENTICATION (PAUT)

Ability of the **device** to authenticate **users**

12-1 Does the **device** support **user/operator**-specific username(s) and password(s) for at least one **user**?	No	__
12-1.1 Does the device support unique **user/operator**-specific IDs and passwords for multiple users?	N/A	__
12-2 Can the **device** be configured to authenticate **users** through an external authentication service (e.g., MS Active Directory, NDS, LDAP, etc.)?	N/A	__
12-3 Can the **device** be configured to lock out a **user** after a certain number of unsuccessful logon attempts?	N/A	__
12-4 Can default passwords be changed at/prior to installation?	N/A	__
12-5 Are any shared **user** IDs used in this system?	N/A	__
12-6 Can the **device** be configured to enforce creation of **user** account passwords that meet established complexity rules?	N/A	__
12-7 Can the **device** be configured so that account passwords expire periodically?	N/A	__

PAUT notes:

13   PHYSICAL LOCKS (PLOK)

Physical locks can prevent unauthorized **users** with physical access to the **device** from compromising the integrity and confidentiality of **private data** stored on the **device** or on **removable media**.

13-1 Are all **device** components maintaining **private data** (other than **removable media**) physically secure (i.e., cannot remove without tools)?	No	__

PLOK notes:

Device Category	Manufacturer	Document ID	Document Release Date
Hearing Aid Analyzer	Audioscan		

Device Model	Software Revision	Software Release Date
Verifit 2	See Page 1 of Users Guide	See Page 1 of Users Guide

	Yes, No, N/A, or See Note	Note #
Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.		

14   ROADMAP FOR THIRD PARTY COMPONENTS IN DEVICE LIFE CYCLE (RDMP)

Manufacturer's plans for security support of 3rd party components within **device** life cycle.

14-1	In the notes section, list the provided or required (separately purchased and/or delivered) operating system(s) - including version number(s).	N/A __
14-2	Is a list of other third party applications provided by the manufacturer available?	N/A __

RDMP notes:

15   SYSTEM AND APPLICATION HARDENING (SAHD)

The **device**'s resistance to cyber attacks and **malware**.

15-1	Does the **device** employ any hardening measures? Please indicate in the notes the level of conformance to any industry-recognized hardening standards.	No __
15-2	Does the **device** employ any mechanism (e.g., release-specific hash key, checksums, etc.) to ensure the installed program/update is the manufacturer-authorized program or software update?	No __
15-3	Does the **device** have external communication capability (e.g., network, modem, etc.)?	Yes __
15-4	Does the file system allow the implementation of file-level access controls (e.g., New Technology File System (NTFS) for MS Windows platforms)?	No __
15-5	Are all accounts which are not required for the **intended use** of the **device** disabled or deleted, for both **users** and applications?	N/A __
15-6	Are all shared resources (e.g., file shares) which are not required for the **intended use** of the **device**, disabled?	Yes __
15-7	Are all communication ports which are not required for the **intended use** of the **device** closed/disabled?	Yes __
15-8	Are all services (e.g., telnet, file transfer protocol [FTP], internet information server [IIS], etc.), which are not required for the **intended use** of the **device** deleted/disabled?	Yes __
15-9	Are all applications (COTS applications as well as OS-included applications, e.g., MS Internet Explorer, etc.) which are not required for the **intended use** of the **device** deleted/disabled?	Yes __
15-10	Can the **device** boot from uncontrolled or **removable media** (i.e., a source other than an internal drive or memory component)?	Yes _7_
15-11	Can software or hardware not authorized by the **device** manufacturer be installed on the device without the use of tools?	No __

7. The device normally boots from internal flash memory. For update purposes the device boots from a connected USB flash drive. Booting from removable media is possible *only* if it contains software supplied by the manufacturer.

SAHD notes:

16   SECURITY GUIDANCE (SGUD)

The availability of security guidance for **operator** and administrator of the system and manufacturer sales and service.

16-1	Are security-related features documented for the **device user**?	N/A __
16-2	Are instructions available for **device**/media sanitization (i.e., instructions for how to achieve the permanent deletion of personal or other sensitive data)?	N/A __

SGUD notes:

Device Category	Manufacturer	Document ID	Document Release Date
Hearing Aid Analyzer	Audioscan		
Device Model	**Software Revision**		**Software Release Date**
Verifit 2	See Page 1 of Users Guide		See Page 1 of Users Guide

Refer to Section 2.3.2 of this standard for the proper interpretation of information requested in this form.	Yes, No, N/A, or See Note	Note #

17   HEALTH DATA STORAGE CONFIDENTIALITY (STCF)

The ability of the **device** to ensure unauthorized access does not compromise the integrity and confidentiality of **private data** stored on **device** or **removable media**.

17-1   Can the **device** encrypt data at rest?   **No**   _8_

STCF notes: 8. The device does not encrypt data and cannot save to encrypted media such as an encrypted USB. Any PHI produced on the device should be de-identified appropriately.

18   TRANSMISSION CONFIDENTIALITY (TXCF)

The ability of the **device** to ensure the confidentiality of transmitted **private data**.

18-1   Can **private data** be transmitted only via a point-to-point dedicated cable?   **No**   __

18-2   Is **private data** encrypted prior to transmission via a network or **removable media**? (If yes, indicate in the notes which encryption standard is implemented.)   **No**   _8_

18-3   Is **private data** transmission restricted to a fixed list of network destinations?   **No**   __

TXCF notes:

19   TRANSMISSION INTEGRITY (TXIG)

The ability of the **device** to ensure the integrity of transmitted **private data**.

19-1   Does the **device** support any mechanism intended to ensure data is not modified during transmission? (If yes, describe in the notes section how this is achieved.)   **No**   __

TXIG notes:

20   OTHER SECURITY CONSIDERATIONS (OTHR)

Additional security considerations/notes regarding **medical device** security.

20-1   Can the **device** be serviced remotely?   **No**   __

20-2   Can the **device** restrict remote access to/from specified devices or **users** or network locations (e.g., specific IP addresses)?   **No**   __

    20-2.1 Can the **device** be configured to require the local **user** to accept or initiate remote access?   **No**   __

OTHR notes: